

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Service Rules for the 698-746, 747-762)	WT Docket No. 06-150
and 777-792 MHz Bands)	
)	
Implementing a Nationwide, Broadband,)	PS Docket No. 06-229
Interoperable Public Safety Network in)	
the 700 MHz Band)	
)	

**COMMENTS OF THE NATIONAL ASSOCIATION
OF TELECOMMUNICATIONS OFFICERS AND ADVISORS,
THE NATIONAL ASSOCIATION OF COUNTIES,
THE NATIONAL LEAGUE OF CITIES, AND
THE U.S. CONFERENCE OF MAYORS
IN RESPONSE TO THE SECOND FURTHER
NOTICE OF PROPOSED RULEMAKING**

Libby Beaty
NATOA
1800 Diagonal Road, Suite 495
Alexandria, VA 22314
(703) 519-8035

Dated: June 20, 2008

TABLE OF CONTENTS

	PAGE
TABLE OF CONTENTS.....	i
SUMMARY	iii
I. INTRODUCTION	1
II. BACKGROUND	3
A. Public Safety Interoperability	3
B. FCC Examines the Problem of Interoperability.....	4
C. Auction 73 and Its Aftermath	6
III. THE SECOND FURTHER NOTICE OF PROPOSED RULEMAKING	7
A. Clarifications and Revisions to the Public Safety Component of the 700 MHz Public/Private Partnership	7
1. Preserve the Public/Private Partnership	7
2. Combining the D Block and Public Safety Spectrum Facilitates Efficiency and Affordability.....	8
3. Provide Flexibility and Local Options.....	9
4. Eligible Users of Public Safety Spectrum in the Shared Network.....	11
5. Potential Users of the Network	14
6. Structure of the Public Safety Broadband Licensee	14
7. Makeup of the Public Safety Broadband Licensee	15
B. Rules Governing the 700 MHz Public/Private Partnership	16
1. Narrowband Relocation	16
2. Geographic Area and Other Rules and Conditions.....	17
3. Interoperability with Existing Networks.....	17
4. Use of Satellite Technology.....	18
5. Access to Public Rights-of-Way	19
6. Penalties for Failure to Provide Emergency Access to Commercial Spectrum	20
7. Auction Reserve Price.....	20
8. Auction Participants and Restrictions.....	21
9. Default Payment.....	22
10. Request for Proposals	22
C. Re-Auction.....	23
IV. CONCLUSION.....	23
APPENDIX – TECHINCAL REPORT	

SUMMARY

Local governments encourage the development of effective and efficient public safety communications infrastructures and strongly support efforts to achieve nationwide interoperability for our first responders. It is without question that the ideal solution for a nationwide, interoperable public safety broadband network would be for the federal government to provide sufficient funding for the construction and maintenance of such a system. But since government funding is not an option, and no other alternative funding means have been identified, the public/private partnership plan is the only viable funding choice available.

One of the most important reasons for preserving the public/private partnership plan is that the combined use of the commercial and public safety spectrum enables the more efficient use of the spectrum and other technical resources. These efficiencies result in significant benefits, including reducing the burden on local jurisdictions that are lacking infrastructure or access to it; increasing build-out feasibility in rural, expensive-to-serve areas; lessening the impact on public rights-of-way; increasing flexibility to serve areas bordered by Canada and Mexico; and maximizing use of spectrum because no guard band between the public safety and commercial allocation would be required.

But while the public/private partnership plan should be retained, we believe improvements can be made. As discussed in the expert Technical Report appended to these Comments, flexibility is critical and local governments must retain the ability to make local and regional decisions concerning data technology deployment that best serves their unique requirements and budget restraints.

It is imperative that the network be designed and implemented using public safety-grade technical standards. There must be a high reliability of the radio signal; sufficient back-up

power; and redundancy of the backhaul connections. And it is critical that there be technical solutions that identify priority users and ensure that critical communications can proceed in an emergency even where networks may otherwise be overwhelmed. Since different jurisdictions will have differing requirements, the network must be sufficiently flexible to add capacity in an *ad hoc* manner.

As efforts continue to resolve the complex problem of public safety interoperability, local governments remain committed to a policy of ensuring that they continue to have the voice, video, and data communications networks required to meet local community needs, ensure the public's safety and convenience, and provide for important and critical communications needs. Public safety agencies must have the option to make local and regional decisions and the ability to choose the solution that best serves their unique requirements and budgets.

With the failure of the D Block to attract a winning bid at Auction 73, the Commission should not rush to take action. Rather, the Commission should adopt new rules and requirements for the public/private partnership plan only after full and fair consideration of the complete record. The development of a nationwide, interoperable public safety wireless broadband network is too important to the nation; and, on behalf of the nation, the Commission is responsible to proceed deliberately.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Service Rules for the 698-746, 747-762)	WT Docket No. 06-150
and 777-792 MHz Bands)	
)	
Implementing a Nationwide, Broadband,)	PS Docket No. 06-229
Interoperable Public Safety Network in)	
the 700 MHz Band)	
)	

**COMMENTS OF THE NATIONAL ASSOCIATION
OF TELECOMMUNICATIONS OFFICERS AND ADVISORS,
THE NATIONAL ASSOCIATION OF COUNTIES,
THE NATIONAL LEAGUE OF CITIES, AND
THE U.S. CONFERENCE OF MAYORS
IN RESPONSE TO THE SECOND FURTHER
NOTICE OF PROPOSED RULEMAKING**

I. INTRODUCTION

The National Association of Telecommunications Officers and Advisors (“NATOA”), the National Association of Counties (“NACo”), the National League of Cities (“NLC”), and the U.S. Conference of Mayors (“USCM”) (collectively, “Commenters”) submit these comments in response to the Second Further Notice of Proposed Rulemaking (“Second FNPRM”), released May 14, 2008, in the above-captioned proceeding.

NATOA’s membership includes local government officials and staff members from across the nation whose responsibility is to develop and administer communications policy and the provision of such services for the nation’s local governments.

NACo is the only national organization that represents county governments in the United States. It serves as a national advocate for counties; acts as a liaison with other levels of government; and provides legislative, research, technical and public affairs assistance to its members.

NLC is the nation's oldest and largest organization devoted to strengthening and promoting cities as centers of opportunity, leadership and governance. NLC is a resource and advocate for more than 1,600 member cities and the 49 state municipal leagues, representing 19,000 cities and towns and more than 218 million Americans.

USCM is the official nonpartisan organization of the nation's 1,183 U.S. cities with populations of 30,000 or more. Its mission is to promote effective national urban/suburban policy, strengthen federal-city relationships and ensure that federal policy meets urban needs.

Local governments encourage the development of effective and efficient public safety communications infrastructures and strongly support efforts to achieve nationwide interoperability for our first responders. As representatives of local governments, we are in the unique position of knowing firsthand how important interoperable communications services are to our police, fire, and other emergency response personnel. We recognize how vital it is that our first responders – from all jurisdictions – have the ability to communicate with one another during times of man-made or natural emergencies.

Local governments manage public safety funding¹ and, as a result, must play a key role in determining how best to create a nationwide, interoperable wireless public safety broadband

¹ Public safety is a significant percentage of most local government budgets. For example, the 2008 budget for the City of Dallas, Texas devotes almost 25% for public safety purposes.
http://www.dallascityhall.com/Budget/adopted0708/Budget_Overview.pdf
Similarly, in 2008 the District of Columbia devotes almost 13% of its budget for public safety.
http://cfo.dc.gov/cfo/frames.asp?doc=/cfo/lib/cfo/budget/2009/executive_summary.pdf

network. A vast majority of all first responders work for local agencies and, without local government input, it is highly unlikely any proposed network will satisfy local and regional first responder needs.² Indeed, “[T]he most effective nationwide public safety network will be one that is developed and deployed with the needs of the local user in mind.”³

It is against this background that we offer the following comments.

II. BACKGROUND

A. Public Safety Interoperability

Public safety interoperability – the ability of a system to work together with another system – has been a problem for years. But the issue took center stage after September 11, 2001, when it became known that New York City police could not communicate by radio with New York City firefighters to warn them of the towers’ looming collapse. The American public was appalled and Congress vowed to remedy the situation.

Recently, it was reported that the 2008-09 fiscal year budget for the city of Los Angeles allocates approximately 71% of its \$7.1 billion for police and fire services. USA Today, *Across the Nation*, June 5, 2008, at p. 5A.

² See, e.g., Comments of the National Association of Telecommunications Officers and Advisors, the National Association of Counties, the U.S. Conference of Mayors, and the National League of Cities, *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102; *Section 68.4(a) of the Commission’s Rules Governing Hearing Aid-Compatible Telephones*, WT Docket No. 01-309; *Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket No. 03-264; *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission’s Rules*, WT Docket No. 06-169; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed May 22, 2007). It has often been said that emergencies are local in nature. Indeed, personnel from the Arlington County, VA Fire Department were at the Pentagon within two minutes after the terrorist attack of 9/11. Arlington County: After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon http://www.arlingtonva.us/Departments/fire/edu/about/docs/after_report.pdf at A-7.

³ See Comments of Motorola, Inc., *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102; *Section 68.4(a) of the Commission’s Rules Governing Hearing Aid-Compatible Telephones*, WT Docket No. 01-309; *Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket No. 03-264; *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission’s Rules*, WT Docket No. 06-169; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed May 23, 2007) at 4.

But nearly four years later, with the devastation of the Gulf Coast by Hurricane Katrina and the interruption and breakdown of public safety communications, we were painfully reminded of how little progress had been made in achieving full public safety interoperability.

B. FCC Examines the Problem of Interoperability

In December 2006, the FCC issued a Ninth Notice of Proposed Rulemaking (“NPRM”) in which the Commission proposed a “centralized and national approach to maximize public safety access to interoperable, broadband spectrum in the 700 MHz band.”⁴ The plan was characterized as a “departure from prior public safety allocations and is designed to speed deployment, decrease costs of roll-out, promote nationwide interoperability and provide a source of funding for constructing a broadband public safety communications network.”⁵

NATOA filed comments in response to the NPRM in favor of the Commission’s goal to achieve nationwide interoperability for our nation’s first responders, but voiced concerns about the exclusion of local communities in the decision-making process, network funding, and build-out requirements.⁶

In April 2007, the FCC released a Report and Order and Further Notice of Proposed Rulemaking (“FNPRM”) in which the Commission “tentatively conclude[d] to redesignate the public safety wideband spectrum for broadband use consistent with a nationwide interoperability

⁴ *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229, Ninth Notice of Proposed Rulemaking (rel. December 20, 2006) (“NPRM”) at ¶ 4.

⁵ *Id.*

⁶ See Comments of the National Association of Telecommunications Officers and Advisors, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed February 26, 2007).

standard” and sought comment on various proposals for the construction of a nationwide public safety broadband network.⁷

Commenters filed initial and reply comments in response to the FNPRM in which we argued for preserving local and regional public safety communications options. In addition, we raised a number of concerns about the various broadband network proposals, including the high cost of building the system and whether potential bidders would be willing to invest in the construction and maintenance of a network that would be subject to preemption during times of emergencies. We raised questions about the terms of the network management agreement and questioned whether public safety entities would be willing to give up their existing systems and subscribe to a new, untested network

In July 2007, the Commission adopted a Report and Order in which it concluded that a public/private partnership represented the best means by which a new, state-of-the-art interoperable public safety wireless broadband network could be built. Among other things, the Report and Order required the winning bidder of the D Block commercial spectrum to negotiate a Network Sharing Agreement (“NSA”) with the Public Safety Broadband Licensee (“PSBL”) to construct a network, consistent with public safety technical requirements, which would permit commercial use of public safety spectrum on a secondary, preemptible basis, along with public safety use of the commercial spectrum during times of emergencies.

⁷ *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102; *Section 68.4(a) of the Commission’s Rules Governing Hearing Aid-Compatible Telephones*, WT Docket No. 01-309; *Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket No. 03-264; *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission’s Rules*, WT Docket No. 06-169; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-72 (rel. April 27, 2007) (“FNPRM”) at ¶ 174-175.

C. Auction 73 and Its Aftermath

Auction 73 for the 700 MHz licenses, including the D Block, began on January 24, 2008, and closed on March 18, 2008. Although Qualcomm was the sole bidder for the D Block, its bid of \$472 million fell far short of the \$1.33 billion reserve price set by the Commission.⁸ The FCC decided not to proceed with an immediate re-auction of the D Block, preferring instead to “provide additional time to consider . . . various options with respect to the D Block spectrum.”⁹

On April 15, 2008, the House Subcommittee on Telecommunications and the Internet held a hearing to review the 700 MHz auction and, more specifically, to examine why the D Block failed to sell. While expressing disappointment with the outcome of the auction, Subcommittee Chairman Edward Markey stated his belief that “pursuing ways for public safety entities and the private sector to partner toward achieving a network that possesses nationwide interoperability and broadband capability remains our best option going-forward on the D-block.”¹⁰

In addition, the FCC’s Office of Inspector General conducted an investigation as to why the D Block failed to attract bidders and concluded that “many layers of uncertainty and risk, and the growing prospect of high network costs . . . were responsible for potential bidders’ decisions not to bid.”¹¹

⁸ Dean Brenner, Vice President of Government Affairs for Qualcomm, stated that the company’s bid was partly to preserve eligibility to bid on the D Block or another block, and partly because it was interested in providing wireless solutions to public safety and wanted its technology used with the shared network.” While the company did not withdraw its bid, it decided against increasing its bid because, in part, it concluded the “build-out requirement was too onerous” and high construction costs. See *Office of Inspector General Report*, from Kent R. Nilsson, Inspector General, to Chairman Kevin J. Martin (OIG rel. Apr. 25, 2008) (*OIG Report*) at 21, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-281791A1.pdf.

⁹ *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229, Second Further Notice of Proposed Rulemaking, (rel. May 14, 2008) (“Second FNPRM”) at ¶ 18.

¹⁰ Press Release of Representative Edward Markey, April 15, 2008, available at <http://markey.house.gov/index.php?option=content&task=view&id=3319&Itemid=125>.

¹¹ *OIG Report* at 26.

III. THE SECOND FURTHER NOTICE OF PROPOSED RULEMAKING

On May 14, 2008, the FCC released its Second Further Notice of Proposed Rulemaking to “consider clarifications and revisions to the public safety component of the 700 MHz Public/Private Partnership that would better promote our public interest goals.”¹² More specifically, the Commission seeks comment on “possible modifications to the various rules governing the D Block licensee and the Public Safety Broadband Licensee within the framework” of the partnership.¹³

A. Clarifications and Revisions to the Public Safety Component of the 700 MHz Public/Private Partnership

1. Preserve the Public/Private Partnership

One of the first issues the Commission seeks comment on is whether it “remains in the public interest to require a public/private partnership between the nationwide D Block licensee and the Public Safety Broadband Licensee for the purpose of creating a nationwide, interoperable broadband network for both commercial and public safety network services.”¹⁴ Considering the fact that Congress has made it clear that government funding of such a vital system is not possible, the answer to this question is yes.

It is without question that the ideal solution for a nationwide, interoperable public safety broadband network would be for the federal government to step up to the plate and provide sufficient funding for the construction and maintenance of such a system. As outlined in the attached Technical Report, this would give the public safety community access to a wireless broadband network constructed to public safety grade specifications without having to compromise its technical and build-out requirements to satisfy the business plan needs of a

¹² Second FNPRM at ¶ 2.

¹³ *Id.* at ¶ 3.

¹⁴ *Id.*

commercial business partner.¹⁵ But, since government funding is not an option, and no other alternative funding means have been identified, the public/private partnership plan is the only viable funding choice available.

2. Combining the D Block and Public Safety Spectrum Facilitates Efficiency and Affordability

One of the most important reasons for preserving the public/private partnership plan is that the combined use of the commercial and public safety spectrum enables the more efficient use of the spectrum and other technical resources. For example, as explained more fully in the attached Technical Report,¹⁶ operating a single network in the combined D Block and public safety spectrum enables sharing of the core infrastructure (antennas, radios, towers, and backhaul systems) rather than duplicative construction of separate commercial and public safety networks. Building two networks would require approximately twice the infrastructure.

The greater efficiency from a single nationwide network where public and private spectrum are combined results in significant benefits, including: (1) reduces the burden on local jurisdictions that lack infrastructure or access to it; (2) increases build-out feasibility in rural, expensive-to-serve areas; (3) lessens the impact on public rights-of-way; (4) increases flexibility to provide spectrum in border areas where spectrum use is limited because of the need to share spectrum with our neighbors in Canada and Mexico; and (5) maximizes use of spectrum because no guard band between the public safety and commercial allocation would be required. As an added benefit, *commercial* D Block customers will receive services from a public safety grade network that is superior to general carrier grade networks because it was designed to meet first

¹⁵ Appended hereto is an expert Technical Report prepared for Commenters by Columbia Telecommunications Corp. ("Technical Report"). Within that report, Dr. Andrew Afflerbach, P.E., of Columbia Telecommunications Corporation describes in detail the differences between a public safety grade and commercial grade wireless network, particularly with respect to design, construction, and operations. Technical Report at 3.

¹⁶ Technical Report at 16-17.

responder needs.¹⁷ Absent the public/private partnership, such benefits may never be fully realized.

Further, to best achieve a cost-effective build-out, it is essential that the plan be premised on standards-based technology rather than proprietary technology. As the attached expert Technical Report describes, expeditious adoption of standards will offer a number of benefits. First, the use of standards-based technology will enable devices to work in any part of the United States, regardless of how they are managed or financed. First responders and their devices will be able to seamlessly roam to any part of the nation over a “Level 6 Interoperability System” as established under U.S. Department of Homeland Security standards, the highest attainable level of data network interoperability. Thus, the use of standards-based technology will make it technologically possible for local first responder agencies to migrate from dated systems to new broadband systems to proceed without delay and without risk to interoperability. And use of such standards will enable economies of scale through efficiency and competition in hardware and a broader base of innovators developing products, which will result in lower cost and higher-performance devices for both commercial and public safety users.¹⁸

3. Provide Flexibility and Local Options

While the public/private partnership plan should be retained, we believe improvements can be made. For instance, as Commenters have repeatedly pointed out, the plan potentially poses a threat to local governments’ ability to make local and regional decisions concerning data technology deployment. We disagree with the Commission’s position that granting flexibility to local governments could hinder efforts to deploy a nationwide, interoperable public safety

¹⁷ *Id.*

¹⁸ *Id.* At 15-16.

broadband network.¹⁹ Flexibility is critical. Public safety entities must continue to have the option to make local and regional decisions and the flexibility to choose the solution that best serves their unique requirements and budgets.²⁰ The Commission should not interfere with the existing options of public safety local and regional decision makers.²¹

Besides the threat to local and regional decision-making, there is also concern that it will take too long to build out a nationwide network of real value. Indeed, these concerns were validated when the current plan's build-out obligations were cited as one of the reasons for the D Block's failure to sell at auction.²²

Realistically, areas of lower population density have few options to meet their mobile data needs in the 700 MHz band until a nationwide network is built throughout their jurisdictions. With a population-based build-out schedule, it is likely that the nationwide network will only be available in those localities with population densities of 10 or more people per square mile. This leaves most of the jurisdictions in the western half of the country, except for the west coast and a few large urban counties, along with some localities in other parts of the country, questioning when – if ever – they will receive nationwide broadband network coverage.

¹⁹ Second FNPRM at ¶ 63.

²⁰ “There must be a process in place that would allow state and local governments to build out their own systems in concert with the national plan in the event the national system schedule does not meet their operational needs.” Comments of the City of Independence, MO, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed May 21, 2007) at 2.

²¹ “The various local and regional areas should be allowed to seek the optimum standards that best fit their operational and financial requirements.” Comments of the City of Tacoma, WA, *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102; *Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones*, WT Docket No. 01-309; *Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket No. 03-264; *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules*, WT Docket No. 06-169; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed May 23, 2007) at 2.

²² *OIG Report at 26.*

Local entities must be permitted to address their own local public safety needs while waiting for the nationwide network to reach their jurisdictions. In reexamining the public/private partnership plan, the Commission should permit public safety entities the ability to make local and regional broadband decisions that best serve their needs and fit within their financial restraints.²³

Specifically, the Commission should ensure that local communities and first responders have a mechanism for decision-making in deployment and operations of the network in their local area. As the expert Technical Report attached describes, public safety communication is inherently local and each community will have unique needs and considerations. Each community should have a say in how the local network meets such key public safety needs including interconnection with existing wired and wireless networks to ensure interoperability with other communications resources;²⁴ rapid authorization and de-authorization of public safety users, so as to respond both to emergency needs for new users and to remove users in the event of a security compromise;²⁵ determination of what constitutes an emergency for purposes of prioritization of public safety traffic;²⁶ and selection of devices and applications so long as they meet standards so as “to serve a range of existing and unanticipated public safety challenges.”²⁷

4. Eligible Users of Public Safety Spectrum in the Shared Network

Section 337(f) of the Communications Act of 1934,²⁸ coupled with the Commission’s eligibility rules for the 700 MHz public safety band,²⁹ limit the use of the public safety spectrum to “public safety services,” which are defined as: (1) services whose “sole or principal purpose of

²³ Current economic factors, not the least of which is fast-rising fuel costs, are adversely affecting public safety budgets and may have a detrimental effect on public safety communications services.

²⁴ Technical Report at 11.

²⁵ *Id.* at 12-13.

²⁶ *Id.* at 15.

²⁷ *Id.* at 13-14.

²⁸ 47 U.S.C. § 337(f).

²⁹ 47 C.F.R. § 90.523.

which is to protect the safety of life, health, or property;” (2) that are provided by “State or local government entities” or “nongovernmental organizations that are authorized by a government entity whose primary mission is the provision of such services;” and (3) that are “not made commercially available to the public by the provider.” As such, the Commission seeks “comment on whether, or to what degree, the Public Safety Broadband Licensee would be statutorily precluded . . . from representing and allowing any entity to use the network for services that are not principally for public safety purposes.”³⁰

Commenters are concerned with any statutory or regulatory interpretations that would allow the PSBL to provide spectrum to entities with “no connection to public safety” or “arguably leave entire pockets within its nationwide service area served only by such non-public safety use.”³¹ Indeed, we agree with the Commission’s statement that “[o]n the policy front, the finite amount of spectrum available to the public safety community – particularly for interoperability purposes – strongly argues against any provision of spectrum access by the Public Safety Broadband Licensee to entities the sole or principal purpose of which is not the protection of the safety of life, health, or property.”³²

At the same time, we are concerned with any interpretations that may limit the ability of all government first responders and emergency support functions to use the network. As the attached expert Technical Report describes, to best facilitate public safety, use of the spectrum must be extended to all government agencies that provide public safety and emergency support services. We cannot obtain interoperability when key responders are not able to access the network. Indeed, the Technical Report notes that in the event of a major metropolitan emergency:

³⁰ Second FNPRM at ¶ 32.

³¹ *Id.*

³² *Id.*

[F]irst responders include not only fire, police, and emergency managers, but also such emergency support functions as:

- Transportation—to operate and monitor the roads for evacuation and emergency passage
- Public health—to care for and track casualties and casualty movements
- Education—to evacuate or protect students, and to establish shelters for displaced persons
- Information technology—to operate the communications networks, distribute backup radios and other gear, and set-up remote emergency operations centers
- Public works—to secure, protect, and distribute critical water and other resources³³

Indeed, the U.S. Department of Homeland Security identifies 15 local Emergency Support Functions (ESFs), including not only fire, search and rescue, and police, but also energy, military, public health, public works, and other agencies that must coordinate responses to emergencies.³⁴

In addition, we are concerned with any interpretations that may limit certain nongovernmental organizations, such as private ambulance services and other critical infrastructure industries, from gaining locally authorized access to the public safety spectrum. Prohibiting network access to such organizations would be directly at odds with the interoperable goals of the nationwide system. By suggesting that these potential users can obtain access to the network through subscription to the commercial versus the public safety service, the Commission fails to recognize the vital communications interaction these organizations currently have and must continue to have with public safety entities during emergencies.³⁵ For this reason, local public safety entities must retain their authority to approve spectrum access to such nongovernmental organizations on a case-by-case basis.

³³ Technical Report at 8-9.

³⁴ <http://www.fema.gov/emergency/nrf/#>.

³⁵ Second FNPRM at ¶ 30.

Commenters are also concerned that the Commission has left the definition of the term “emergency” to be negotiated between the PSBL and the D Block licensee. Certainly local public safety officials make this determination on a daily basis, subject to the unique needs of their respective communities. As such, we believe that a single definition by a national entity may be inappropriate and that local input is essential.

5. Potential Users of the Network

It will be difficult to accurately predict what public safety entities will subscribe to the proposed new network.³⁶ The answer to this question will depend in large part on the network’s build-out schedule and the pricing scheme that is eventually put into place. Adoption rates will also be affected by the network’s available speeds, service features, technical features, etc. But it is safe to say that some jurisdictions simply will not use the network. For example, in earlier comments, the city of Philadelphia stated that it “does not itself foresee a need to utilize the services of a nationwide broadband licensee, but can envision a greater use for regional systems.”³⁷

6. Structure of the Public Safety Broadband Licensee

Consistent with our earlier comments, we continue to believe that “no commercial interest may be held in the Public Safety Broadband Licensee,³⁸ that no commercial interest may participate in the management of the licensee, and that the licensee must be a non-profit

³⁶ Second NRPRM at ¶ 33.

³⁷ Comments of the City of Philadelphia, PA, *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102; *Section 68.4(a) of the Commission’s Rules Governing Hearing Aid-Compatible Telephones*, WT Docket No. 01-309; *Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket No. 03-264; *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission’s Rules*, WT Docket No. 06-169; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed May 23, 2007) at 2.

³⁸ On November 19, 2007, the Public Safety Spectrum Trust (“PSST”) was granted the Public Safety Broadband License. See *OIG Report* at 5.

organization.”³⁹ These conditions are necessary to ensure that the PSBL acts solely in the interest of public safety entities nationwide.

And while we agree that the PSBL “not obtain debt or equity financing from any source, whether debt or equity, unless such source is also a non-profit entity,”⁴⁰ it is important that the PSBL have sufficient resources to carry out its duties.⁴¹ We believe that government funding of the PSBL is the best option to preserve the licensee’s independence from commercial interests. We are encouraged by Congressional efforts, such as Representative Jane Harman’s proposed legislation,⁴² that would provide operational funding for the PSBL.

7. Makeup of the Public Safety Broadband Licensee

Commenters have previously raised concerns as to whether a single public safety licensee could properly represent the varied interests of public safety entities across the nation.⁴³ And while we are supportive of the concept that the PSBL be “broadly representative of the public safety community,”⁴⁴ we are concerned that local governments are not adequately represented by the current makeup of the licensee.⁴⁵ As stated in the Introduction, a vast majority of the

³⁹ Second FNPRM at ¶ 39.

⁴⁰ *Id.* at ¶ 40.

⁴¹ For more information regarding how the lack of funding for the PSBL may have adversely affected Auction 73, see *OIG Report*.

⁴² Rep. Harman’s proposed legislation, the “Public Safety Broadband Authorization Act of 2008” (H.R. 6055), would, among other things, “establish a grant program to fund administrative and operational costs” of the public safety broadband licensee. However, it is unclear whether the bill’s \$1 million a year grant for fiscal years 2009 and 2010 would be sufficient to fully fund the licensee’s costs.

⁴³ See Comments of the National Association of Telecommunications Officers and Advisors, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed February 26, 2007).

⁴⁴ Second FNPRM at ¶ 46.

⁴⁵ The PSST’s Board of Directors consists of representatives from the following organizations: American Association of State Highway and Transportation Officials; American Hospital Association; Public-Safety Communications Association; Forestry Conservation Communications Association; International Association of Chiefs of Police; International Association of Fire Chiefs; International City/County Management Association; National Association of State Emergency Medical Services Officials; International Municipal Signal Association; National Association of State 9-1-1 Administrators; National Emergency Management Association; National Emergency Number Association; National Fraternal Order of Police; National Governors Association; and National Sheriffs’ Association.

nation's first responders are employed by local government agencies. Yet, the board lacks representation from any national association representing local government elected officials, such as the National Association of Counties, the National League of Cities, and the U.S. Conference of Mayors. Considering the fact that decisions regarding whether to participate in a nationwide public safety broadband network will be made by local elected officials and further that local services, systems, property, and personnel will be directly affected by the construction of a nationwide public safety broadband network, the exclusion of such representation deprives the PSBL of the insights and experience of elected local government officials that represent the entities the PSBL is charged to serve and is therefore inexcusable.

To the extent that the Commission is amenable to taking steps to help alleviate these concerns, we recommend, as we have before, that the PSBL expand or modify the current make-up of its board to ensure representation from city and county elected officials and from the national organizations that represent them.

B. Rules Governing the 700 MHz Public/Private Partnership

The Commission must craft new rules that will appeal to both commercial interests and public safety concerns. As we saw from Auction 73, this will be a difficult path to tread.

1. Narrowband Relocation

The current relocation reimbursement cap of \$10 million is simply inadequate to compensate all jurisdictions that may be adversely affected by the relocation of narrowband services.⁴⁶ Facing increasing burdens on limited budgets, local governments should not be forced to use scarce resources to pay relocation costs that will benefit private companies. Therefore, the Commission should remove the \$10 million cap and the winning bidder of the D Block should be responsible for reimbursing local jurisdictions their reasonable relocation costs.

⁴⁶ Second FNPRM at ¶ 180.

We do not believe that deadlines or complex rules are necessary to achieve the relocation goals; on the contrary, those local governments affected are self-motivated toward the relocation's goals and ask only for reasonable compensation for the cost of moving.

2. Geographic Area and Other Rules and Conditions

A single, nationwide license is consistent with Congressional intent and the need of our nation's public safety entities. The Commission should not prematurely abandon the nationwide model until it has adequately explored the potential of the public/private partnership. It is therefore premature to consider alternative approaches such as regional or split licenses given that the Commission has not yet explored the auction market for the D Block under revised rules.

3. Interoperability with Existing Networks

It is imperative that the new network be able to interoperate with legacy networks, and that the D Block licensee facilitate interconnection of the new network to existing local communications resources.⁴⁷ Therefore, the Commission should consider the various means by which this may be accomplished.⁴⁸ Indeed, "it is operating procedures, protocols, and regional agreements that create real interoperability."⁴⁹ However, no public safety entity should be penalized in the event its existing system cannot interoperate with the new, nationwide system.

⁴⁷ Technical Report at 11-12.

⁴⁸ "Interoperability can be achieved without the Commission mandating a single broadband technology and limiting the spectrum to only a nationwide network. . . . The City of Fort Lauderdale therefore urges the Commission to allow public safety agencies and Regional Planning Committees to make local/regional decisions on the 700 MHz public safety data spectrum, which give them the flexibility to deploy high-speed data solutions that best meet their budget and operational requirements." Comments of the City of Fort Lauderdale, FL, *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150; *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules*, WT Docket No. 06-169; *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed May 23, 2007) at 2-3.

⁴⁹ Comments of the City of Philadelphia, PA, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed February 26, 2007) at 5.

The goal in this proceeding should be to ensure that the D Block licensee constructs a useful and attractive network for public safety use – not to penalize localities that had the foresight and resolve to build their own networks to protect the public’s health, safety, and welfare. As we have stated previously, there should be no mandatory requirement that public safety entities use the proposed network, but there must be a requirement that provides for interconnection of existing networks with the new network. And while the Commission could provide incentives for public safety use of the network, it should not impose penalties on jurisdictions that opt out so long as the alternative choices made by those jurisdictions are standards-based and interoperable with the nationwide network.

Local governments should always retain the right to make decisions about public safety communications based on local public safety considerations. If the Commission imposes penalties on those communities that choose not to purchase services from the public/private partnership, such an approach will be defeating of public safety and will force localities to become unwilling users of a network they do not want or need. In essence, such a rule would amount to the Commission forcing local first responders to become revenue sources for for-profit commercial carriers.

4. Use of Satellite Technology

While satellite technology may be useful in providing service to some hard-to-reach areas of the country, it is expensive and has lesser capabilities than terrestrial-based broadband data networks such as that contemplated by this proceeding. As the attached Technical Report makes clear, capacity in a satellite network is shared by a large potential number of users and may be overwhelmed when a significant fraction of those users needs to access the system at once.

Relative to a terrestrial network, satellite capacity is scarce and expensive. Satellites are limited in their ability to provide broadband data services, such as high resolution images or video.⁵⁰

In light of these limitations, Commenters note that: “[s]atellite communications--though essential as a *backup* to terrestrial-based emergency communications systems—cannot *substitute* for a capable terrestrial-based wireless public safety network.”⁵¹ As such, satellite service should not be counted when calculating the network’s goal of reaching 99.3% of the population within 10 years and should not be available to the D Block licensee as a mechanism by which to escape build-out requirements of the D Block license.⁵²

5. Access to Public Rights-of-Way

Local jurisdictions have the right and responsibility to manage their public rights-of-way to protect public health and safety. As such, they must continue to have the ability to manage public property through the permitting process, zoning enforcement, safety code enforcement, and other traditional exercises of local police powers. The Commission does not have the authority and must not take any action that would adversely affect the rights-of-way management authority of local communities and the right of local communities to make their own decisions about how to utilize their resources.

Further, mandatory access to public facilities could be antithetical to public safety and homeland security. We strongly protest the idea that commercial entities and their employees should have mandatory access to critical municipal infrastructure and resources when such access may put at risk the very security for which local governments strive.

⁵⁰ Technical Report at 9-10.

⁵¹ *Id.*

⁵² Second FNPRM at ¶99.

6. Penalties for Failure to Provide Emergency Access to Commercial Spectrum

It is important that the Commission establish rules requiring compliance with emergency access obligations and clarify the penalties to be imposed on the D Block licensee in the event public safety entities are effectively denied emergency access to the commercial spectrum, either intentionally or as a result of poor engineering or operations. While fines may deter smaller operators from doing so, larger providers may opt to pay a fine rather than taking action that may result in interrupting broadband service to their commercial subscribers. The Commission should take steps to adopt rules that will mandate the imposition of substantial fines, immediate license revocation, or other penalties to ensure that public safety entities will have full access to the spectrum needed during times of emergencies. In addition, as the attached Technical Report describes, an ongoing testing mechanism will be critical to verify that the system is engineered and maintained to properly enable public safety prioritization in the event of emergency.⁵³ Through testing and clear statement of penalties, the Commission can ensure before-the-fact compliance with, and verification of, public safety prioritization—rather than after-the-fact enforcement.

7. Auction Reserve Price

Auction 73 raised over \$19 billion in winning bids, nearly double the amount the Office of Management and Budget had estimated the auction would raise. As a result, Commenters strongly suggest that the Commission reject setting a reserve price for the re-auction of the D Block.⁵⁴ Because of the expense the winning bidder will incur in building out a new, nationwide public safety broadband system, the elimination of a high reserve price could serve to encourage potential bidders to take part in the re-auction of the spectrum. However, our position on this

⁵³ Technical Report at 18.

⁵⁴ Second FNPRM at ¶ 164.

issue is conditioned to the extent that the Commission proceeds with the public/private partnership.

8. Auction Participants and Restrictions

While we are supportive of efforts to broaden auction participation by all parties, especially those “that do not already have significant access to 700 MHz band spectrum or other spectrum potentially suitable for the provision of mobile wireless broadband services,”⁵⁵ we do not believe the Commission should impose any restrictions on eligibility to bid on the D Block license. However, this position applies only to the extent that the D Block license retains the requirement to construct an interoperable public safety broadband network.⁵⁶

The Commission can take other actions to further competitive access to the 700 MHz spectrum. For example, the Commission could provide that the D Block license may be held by a conglomerate of smaller operators, which would require the relaxation of the Commission’s anti-collusion rules.

Further, as long as the Commission maintains the public/private partnership requirement on the D Block, we are supportive of the Commission’s preemption of the impermissible material relationship rule.⁵⁷ Doing so may very well help smaller companies bid for the spectrum.

⁵⁵ Second FNPRM at ¶ 157.

⁵⁶ To the extent the Commission acts to auction the D Block without any public safety broadband requirements, we have no comment on this issue.

⁵⁷ “Under this rule, except for cases where specifically grandfathered, an applicant or a licensee is considered to have an “impermissible material relationship” if it has entered into arrangements with one or more entities for the lease or resale (including wholesaling arrangements) of more than 50 percent of the spectrum capacity, and is therefore ineligible for designated entity benefits.” See Muncie Free Press, *FCC Waives Portions of “Designated Entities” Eligibility Rules for Upper 700 MHz Block License*, November 16, 2007, available at <http://www.munciefreepress.com/node/18229>.

9. Default Payment

The Commission's default penalties have been cited by some as one of the reasons for the failure of the D Block to attract a winning bidder in Auction 73. With the degree of uncertainty surrounding the network management agreement, large monetary penalties were of great concern to potential bidders. However, with the Commission seeking to ensure more detail as to the service and technical requirements of the shared network, along with the possible elimination of the high reserve price, bidders should be less reticent of the Commission's default penalty in this matter. However, it is important that the winning bidder be obligated to negotiate in good faith and failure to do so may result in significant penalty or forfeiture.

10. Request for Proposals

The Commission asks whether it would be feasible to use requests for proposals ("RFPs") to "effectively match the needs of public safety users with the capabilities of potential service providers while still meeting [its] obligation under the Act to assign the D Block by competitive bidding."⁵⁸ Commenters are in favor of such an approach. However, the Commission should be cautious and not adopt specifications that would too closely tailor the RFP to a particular provider.

In earlier comments, Verizon argued that such a process "is the best way to generate a wide range of approaches to meet public safety's needs"⁵⁹ and we agree. Considering earlier efforts by the PSBL to engage potential bidders in discussing how such a network could be built, and the criticism that such meetings generated, the use of an RFP would help ensure that all parties share a level playing field and that respondents' bids are public rather than secret.

⁵⁸ Second FNPRM at ¶ 188.

⁵⁹ Comments of Verizon Wireless, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229; *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86 (filed February 26, 2007) at 4.

C. Re-Auction

It is likely the Commission will receive comments arguing that the D Block be re-auctioned with no restrictions. But doing so, as discussed above, will leave public safety with no viable funding alternative for the construction of a nationwide, interoperable network. The Commission should not permit such a scenario and, indeed, doing so would be contrary to Congress' stated goal of achieving nationwide public safety interoperability.

Further, we believe that it is premature for the Commission to now determine its course in the future event that the re-auction fails. Rather, the Commission should dedicate its efforts to ensuring that this essential proceeding is successful and that feasible commercial and public safety networks result from the proceeding. Moreover, we are concerned that the Commission not take a defeatist attitude towards the potential of the public/private partnership, or that it create a negative self-fulfilling prophecy. There should be no expectation created that the D Block spectrum will become available without public safety requirements should the re-auction fail.

IV. **CONCLUSION**

As we work towards solving the complex problem of public safety interoperability, Commenters remain committed to a policy of ensuring that local governments continue to have the voice, video, and data communications networks they require to meet local community needs, ensure the public's safety and convenience, and provide for important and critical communications needs. Public safety agencies must have the option to make local and regional decisions and the ability to choose the solution that best serves their unique requirements and budgets.

With the failure of the D Block to attract a winning bid at Auction 73, the Commission should not rush to take action. Rather, the Commission should adopt new rules and requirements for the public/private partnership plan only after full and fair consideration of the complete record. The development of a nationwide, interoperable public safety wireless broadband network is too important to the nation; and, on behalf of the nation, the Commission is responsible to proceed deliberately.

Respectfully submitted,

Libby Beaty
NATOA
1800 Diagonal Road, Suite 495
Alexandria, VA 22314
(703) 519-8035
June 20, 2008

An Engineering Assessment
of Select Technical Issues
Raised in the Re-auction of the D Block Spectrum

Prepared for
National Association of Telecommunications
Officers and Advisors
National League of Cities
National Association of Counties
U.S. Conference of Mayors

June 2008

Prepared by
Andrew Afflerbach, Ph.D., P.E.
Director of Engineering



Columbia Telecommunications Corp • 10613 Concord Street • Kensington, MD 20895
301.933.1488 • www.CTCnet.us

Table of Contents

I.	Introduction.....	1
II.	To Facilitate Public Safety, the Network Must Be Public Safety Grade	2
A.	<i>Comparison between commercial and public safety grade broadband wireless networks</i>	<i>2</i>
B.	<i>A public safety network requires capacity in any emergency.....</i>	<i>6</i>
C.	<i>A public safety network requires sufficient capacity and RF coverage.....</i>	<i>7</i>
C.	<i>A public safety network must provide access for all government public safety and emergency support users.....</i>	<i>8</i>
D.	<i>Because of technological limitations, satellite communications cannot substitute for a terrestrial public safety wireless in the 700 MHz spectrum.....</i>	<i>9</i>
III.	There Must be a Mechanism for Local Decision-Making on Technical/ Engineering Matters 10	
A.	<i>Connectivity between the wireless network and the first responder network.....</i>	<i>11</i>
B.	<i>Control of access and authentication and security</i>	<i>12</i>
C.	<i>Local first responder selection of devices</i>	<i>13</i>
D.	<i>Local first responder selection of applications</i>	<i>14</i>
E.	<i>Local determination of an emergency.....</i>	<i>15</i>
IV.	Expeditious Adoption of Open Standards Will Enable Efficiencies, Cost Savings, and Local Deployment Without Delay--and Without Compromising Interoperability	15
V.	Combined Spectrum Will Boost Spectral and Cost Efficiencies.....	16
VI.	Verification of Public Safety Compliance Will Be Essential	18

Table of Figures

Figure 1: Typical Public Safety Network Structure	4
Figure 2: Comparison of Public Safety Grade and Commercial Grade Facility	5
Figure 3: Emergency Scenario at Commercial Wireless Cell.....	7
Figure 4: Phases in Network Design/Build and Network Operation	11
Figure 5: Public Safety Grade Broadband Network Facility	12
Figure 6: Utilization of Public Safety Broadband Network.....	13

I. Introduction

This Report presents the results of an engineering evaluation of some of the issues raised by the Second Further Notice of Proposed Rule Making with respect to the D Block of 700 MHz spectrum currently under consideration for re-auction by the Federal Communications Commission.

This Report was prepared in June 2008 by Columbia Telecommunications Corporation (CTC) at the request of the National Association of Telecommunications Officers and Advisors, the National League of Cities, the National Association of Counties, and the U.S. Conference of Mayors.

CTC was requested to prepare an engineering assessment of technical issues underlying the question of how best to structure the D and public safety blocks of spectrum in the 700 MHz band to best serve the goals of deployment of a nation-wide interoperable, broadband, wireless, public safety network. Specifically, this Report:

1. Describes the local input and considerations that will be essential to preserve public safety utility. To successfully facilitate public safety, the model the FCC adopts must enable public safety grade communications as they are traditionally understood, so that first responders and local emergency support workers will make use of and benefit from the network.
2. Describes the need for formalized mechanisms for local decision-making on technical/engineering matters such as interconnectivity with existing local networks and capability to rapidly authorize and de-authorize users.
3. Describes how government public safety and emergency support users must all have access to the network in order for true interoperability to be achieved.
4. Recommends adoption of an immediate skeleton technical standard that will enable pending local efforts to proceed without delay and without risk to interoperability.
5. Describes how any plan that makes joint use of both blocks of spectrum under consideration is advisable from a technical standpoint because the combination of public safety and D Block spectrum enables more efficient use of spectrum and other technical resources. This combined use of spectrum is advisable regardless of business model.
6. Advises selection of a standards-based technology rather than a proprietary technology because such a selection will facilitate both efficiency and competition in hardware vendors -- and will make devices more affordable for both public safety and commercial users.

7. Describes how verification of public safety requirements will be essential because, absent verification, risk exists of mistaken or intentional abrogation of public safety requirements. In particular, testing requirements are essential in an environment in which local public safety has less control than in the traditional public safety communications environment.

II. To Facilitate Public Safety, the Network Must Be Public Safety Grade

The 700 MHz spectrum offers the first opportunity for first responders to use a *public safety-grade* broadband wireless data network, which is far superior for public safety needs (reliability, availability, security) than are commercial grade networks.

This section of this report describes the differences between a public safety grade wireless network and a commercial grade wireless network. It describes why it is critical that the contemplated public safety broadband network be designed and implemented to the public safety standard described above.¹ It also describes the need for local public safety practitioners to have input into design and implementation and sufficient control of their operating environment.

Some first responders do already have wireless broadband devices--in jurisdictions that can afford the recurring costs of such services.² As useful as these services are, however, *they are not public safety grade*—they do not run on hardened networks that are designed to withstand certain kinds of disasters—and they may or may not enable public safety prioritization in the event of emergency.

A. Comparison between commercial and public safety grade broadband wireless networks

¹ For example, David Boyd, the head of Safecom, a Homeland Security program dedicated to public safety interoperability, has noted that commercial networks cannot withstand the worst of disasters. Mr. Boyd recognized that the private sector doesn't have incentive to build hardened networks that include redundancy and other safeguards—the kind of features that are essential in major emergencies, “exactly when communications is needed most.” Government Executive Magazine, “Missed Signals,” <http://www.govexec.com/features/0206-01/0206-01s2.htm>, accessed June 15, 2008.

² It is increasingly clear that police, fire, and emergency services responders have growing critical needs for broadband wireless data for such applications as:

- computer assisted dispatching (CAD)
- geographic information systems (GIS)
- incident management tools (such as WebEOC)
- interactive video
- video from live incidents.

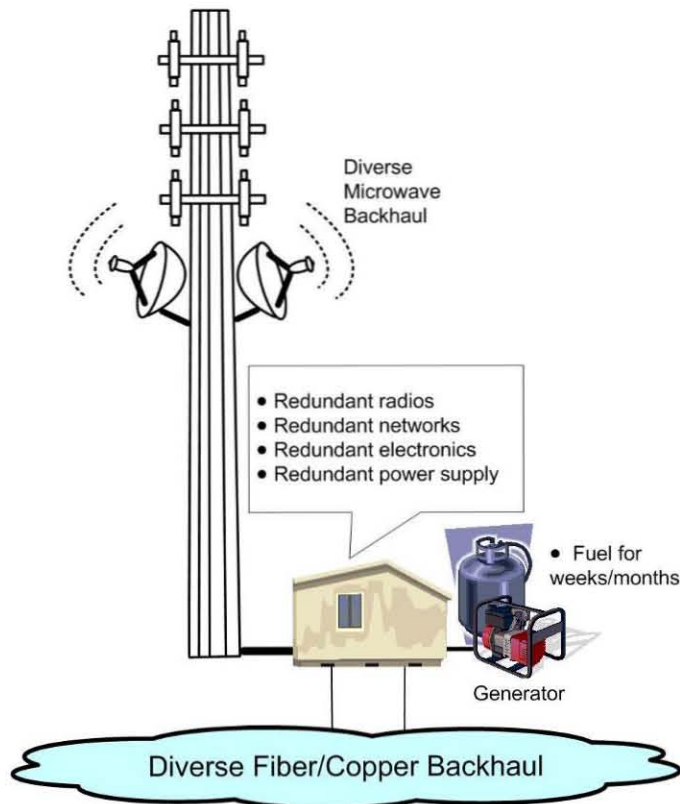
Commercial broadband data networks are designed, built, and operated according to commercial standards of reliability and integrity. There are no formal technical requirements for the performance and reliability of these commercial networks, other than recently adopted FCC requirements for eight hours of backup power at antenna sites. There are no enforceable limits on acceptable outages, guarantees of data rates, or guarantees of performance in emergencies or at the locations of incidents.

Many of the technologies used in commercial data networks have the capability to prioritize certain types of traffic—for example, convey sensitive voice and video applications with higher priority than non-time-critical traffic, such as file transfers. This capability, if implemented, can potentially prioritize public safety applications over others. However, in order for commercial networks to compare to public safety grade networks, the prioritization scheme must keep public safety users on the network in an emergency, even in a scenario where there is extremely high commercial data usage.

In other words, first responders may be no better off than any other user in the event of an incident requiring emergency response—and public safety is therefore compromised relative to use of a network engineered for public safety needs and to public safety standards.

A public safety grade network is different in many significant respects from a commercial grade network. It is designed with a high reliability of the radio signal (availability). It has on-site backup power of weeks or months at all sites. It typically has redundancy of the backhaul connection between an antenna site and the core infrastructure, with multiple fiber, microwave, or copper communications connections. There is redundancy of components at the cell site and at the core. Figure 1 illustrates this general configuration.

Figure 1: Typical Public Safety Network Structure

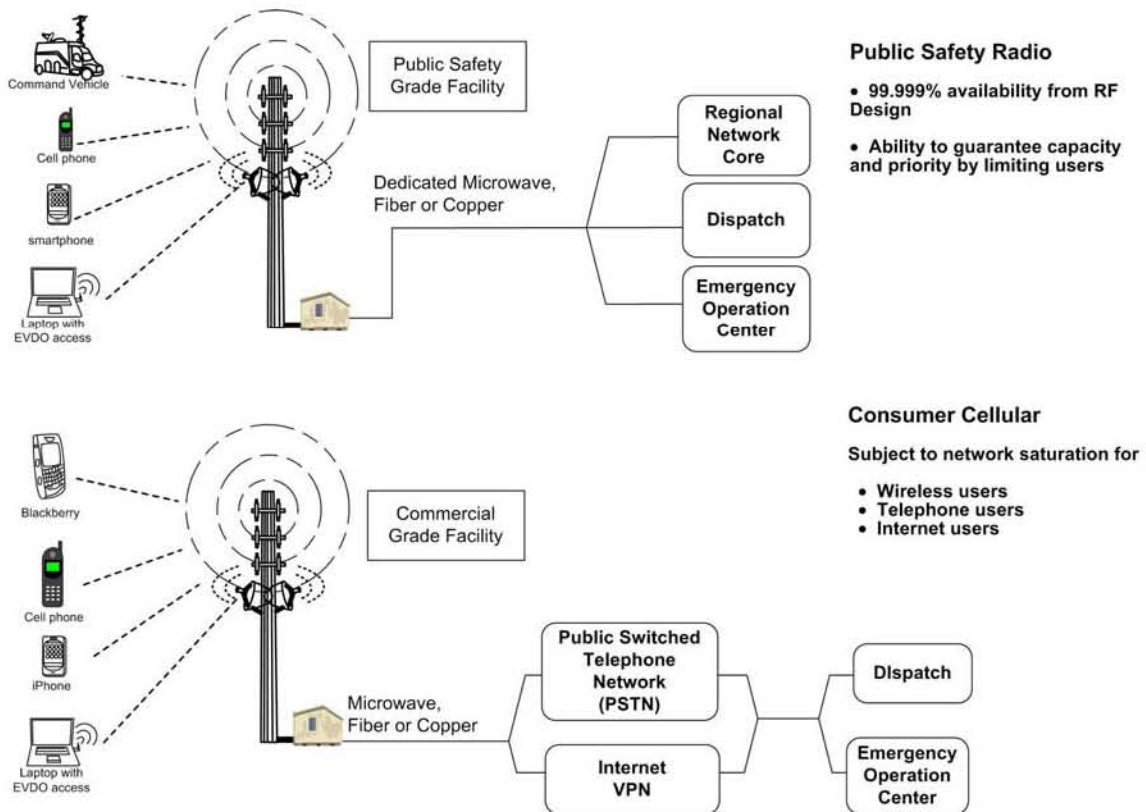


Public safety networks also have the distinguishing characteristic that local government staff performs the following key tasks, all of which help secure the network and maintain its status as public safety grade:

- Determine who has access to the sites and knowledge of the infrastructure.
- Determine how many individuals obtain devices and how they connect to the network.
- Manage capacity usage on the network with a range of techniques, including directly assigning and managing channels and limiting the number of individuals with access to the network.
- Select and authorize all accounts and devices.
- In the event of a security or other event, can immediately disconnect a user or de-authorize a device.
- In the event that a base station or core component fails, the devices at an incident site can “speak” directly with each other in a walkie-talkie mode.

Figure 2 illustrates the contrasting characteristics of public safety grade and commercial grade facilities.

Figure 2: Comparison of Public Safety Grade and Commercial Grade Facility



Justifiably, first responders do not introduce new technologies or make significant changes in their practices unless the change represents a demonstrable and reliable improvement. If a public safety broadband network does not significantly address the technical limitations of the commercial networks, at least three negative outcomes are likely:

1. First responders will still not have interoperability or a reliable broadband data solution they can use in an emergency, significantly impairing their ability to perform in a critical situation such as 9/11 or Hurricane Katrina.
2. Some localities may choose not to adopt this technology because of its limitations.
3. Even where localities do adopt the technology, many first responders may opt to stay with familiar commercial solutions that they understand, despite their technical limitations.

If, therefore, the nationwide network is to succeed in addressing local public safety needs, the public safety elements of the FCC's original vision should not be diluted.

B. A public safety network requires capacity in any emergency

One of the key limitations of commercial networks is the challenge of adequately prioritizing public safety traffic. There are many technical solutions that identify priority users and ensure that critical communications can proceed in an emergency where networks may be overwhelmed. However, it is critical that the solution that is chosen will address all of the areas that could impact these communications.

A workable prioritization scheme³ addresses:

1. Ensuring that critical users remain continuously connected even as many critical and non-critical users attempt to use the network and the network becomes saturated.
2. Ensuring that critical users are able to newly connect to the network, regardless of use or saturation and even if non-critical users must be disconnected or limited.
3. Providing sufficient priority to key applications such as voice and video that would suffer in the event of interruption.
4. Enabling critical users to remain connected as they roam from cell to cell.
5. A prioritization scheme among the first responders, so that in the event of saturation by the first responders themselves, the incident commander can prioritize particular applications or particular groups of responders.
6. Sufficient backhaul capacity to support all potential public safety users.
7. Sufficient connectivity to outside resources that users require, such as the Internet, public switched telephone system, and public safety applications and databases

Many of these items are being addressed by Multimedia Prioritization Services (MPS) under development.⁴ The existing Wireless Priority Service (WPS) implemented in recent years enables first responders to enter a code to go to the “front of the line” to connect their wireless phones as soon as capacity becomes available.⁵ However, this mechanism does not provide any options in the event the cell is already fully used. Moreover, it was designed for voice services and does not extend to broadband data services.

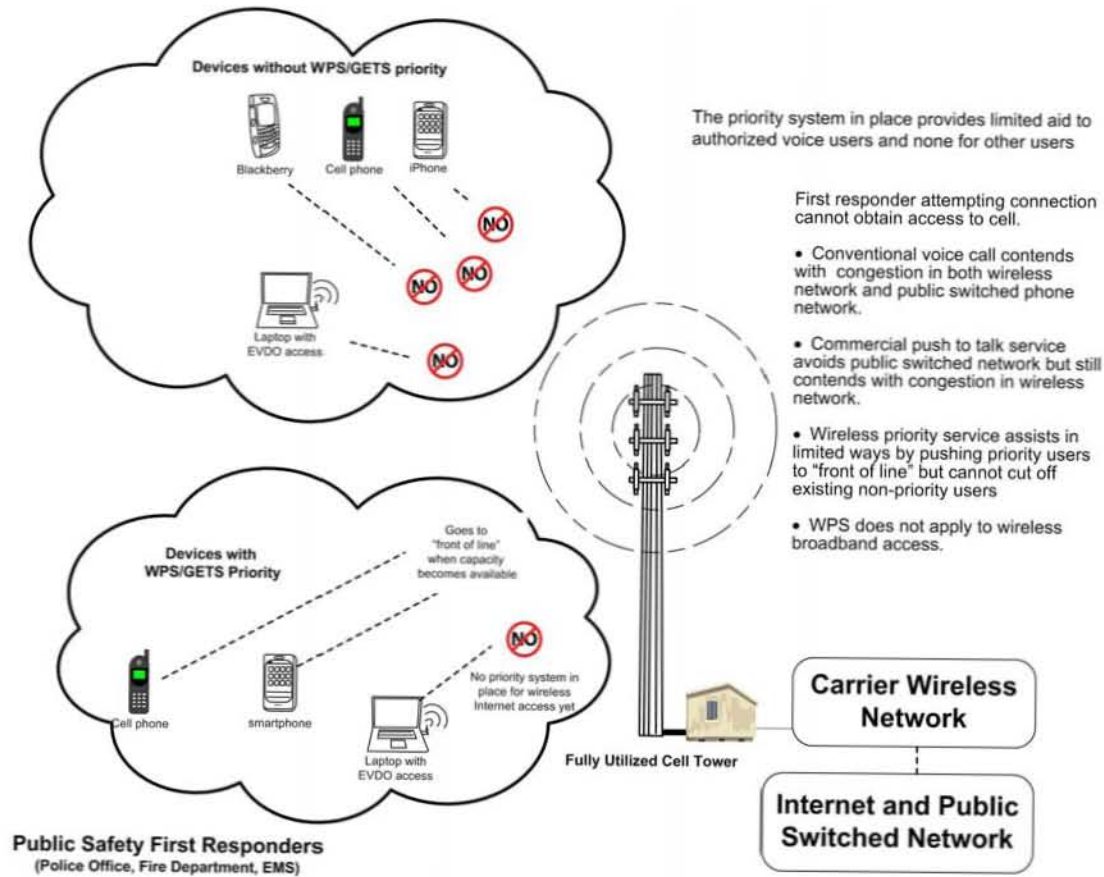
Figure 3 illustrates how WPS works during times of emergency.

³ “Prioritization” refers to the mechanism to allocate a party of higher priority a higher level of service availability so that their transmissions are given higher priority for continuous connectivity than lower-priority parties.

⁴ <http://www.3gpp.org/ftp/specs/html-info/22153.htm>, accessed June 19, 2008, references a GSM based standard under development; a similar standard is in process for other broadband wireless technologies.

⁵ See <http://wps.ncs.gov>, accessed June 15, 2008

Figure 3: Emergency Scenario at Commercial Wireless Cell



There are multiple technical solutions to provide an acceptable prioritization scheme. One possibility is to dedicate spectrum within the network for the first responders, both for their data usage and in the control signaling for authentication and handoff between cells. Another may be to identify critical users by device and assign their communications a higher priority, provided that the solution has a way to authenticate new critical users, continue operating in a saturated environment, and limit or terminate non-critical communications as necessary.

C. A public safety network requires sufficient capacity and RF coverage

In any event, the FCC's solution must provide sufficient capacity for an emergency first-responder scenario. The requirements depend on the number of responders, the types of application used, and the physical distribution of responders. It also depends on the resources and emergency plans of the first responders

Different jurisdictions and different geographic areas will have different requirements. Moreover, those jurisdictions may need to modify those requirements in an actual emergency, where the geographic distribution may be different from any plan, and out-of-area responders (neighbors, state, federal) may take part. As a result, the network will need to be sufficiently flexible to add capacity in an ad hoc manner.

In any case, designing the capacity in coordination with public safety officials will provide a predictable baseline of capacity and RF coverage. This knowledge baseline is the norm in public safety radio communications. The network may not provide perfect coverage for all conceivable locations, but the limitations of the network will at least be known to practitioners and incorporated into their planning and training. The localities may be able to proactively address limitations of the network through zoning practices and their own augmentation of the network—for example, by requiring owners of large buildings to install amplifiers.

In order to accommodate the capacity requirements, it is recommended that the designers of the public safety broadband wireless network coordinate with local public safety officials to:

1. Design capacity, working with both the day-to-day and disaster scenarios of numbers of users and applications used.
2. Develop an initial service and capacity footprint, with the ability to enhance capacity in later phases of deployment.
3. Determine how additional capacity will be made available in an emergency—for example, by terminating non-critical users.
4. Determine how capacity in particular geographic areas can be enhanced in an emergency, for example, by deploying cells on wheels. Local emergency commanders should be able to own and operate their own mobile cells or call on cells from the operator in a reasonable amount of time.

C. A public safety network must provide access for all government public safety and emergency support users

To best facilitate public safety, use of the spectrum must be extended to all government agencies that provide public safety and emergency support services.

True interoperability includes a wide range of first responders and emergency support functions. In the event of major metropolitan emergency, the first responders include not only fire, police, and emergency managers, but also such emergency support functions as:

- Transportation—to operate and monitor the roads for evacuation and emergency passage
- Public health—to care for and track casualties and casualty movements
- Education—to evacuate or protect students, and to establish shelters for displaced persons

- Information technology—to operate the communications networks, distribute backup radios and other gear, and set-up remote emergency operations centers
- Public works—to secure, protect, and distribute critical water and other resources

It is not only localities that recognize that the integrated nature of emergency response extends to multiple types of responders. The U.S. Department of Homeland Security identifies 17 Emergency Support Functions (ESFs), including not only fire, EMS, and police, but also energy, military, public health, public works, and other agencies that must coordinate responses to emergencies.

D. Because of technological limitations, satellite communications cannot substitute for a terrestrial public safety wireless in the 700 MHz spectrum

Satellite communications provide a significant capability and should be part of any jurisdiction's emergency plans. In a regional emergency where local power, radio towers, and communications utilities are severely compromised (as occurred during and after Hurricane Katrina) satellites may provide the only working technology. There are also portions of the country that are so remote or so distant from significant infrastructure that the only cost-effective and flexible means of communicating is to use satellites. The military is a significant user of satellite technology, and it is one of the only effective ways to flexibly provide capacity in oceans and remote theaters of operations across the world.⁶

It is important to note that satellites have significant limitations as well. Most importantly, capacity in a satellite network is shared by a large potential number of users and may be overwhelmed when a significant fraction of those users needs to access the system at once. Individual satellites fulfill the role of wireless base stations—but while hundreds or thousands of base stations would be built in a terrestrial network, only dozens of satellites would be built in a satellite constellation, placing significant demands on each component of the satellite system. Relative to the terrestrial network, satellite capacity is scarce and expensive.

Because of the limited capacity, satellites must be used more judiciously than capable terrestrial networks. They are limited in their ability to provide images and video.

Because of the delay in signal propagation, some data applications will need to be modified, or may not be effective. Some email applications and services are engineered for short delays and will need to be modified by their programmers not to “time out” over

⁶ Maryann Lawlor, “Wideband Global Connection Goes Live,” Signal Magazine, Armed Forces Communications and Electronics Association, June 2008, http://www.afcea.org/signal/articles/templates/signal_connections.asp?articleid=1631&zoneid=220, accessed June 18, 2008.

a satellite link. Some multimedia applications will not work effectively when satellite users are delayed relative to other users.

Satellite communications—though essential as a *backup* to terrestrial-based emergency communications systems—cannot *substitute* for a capable terrestrial-based wireless public safety network.

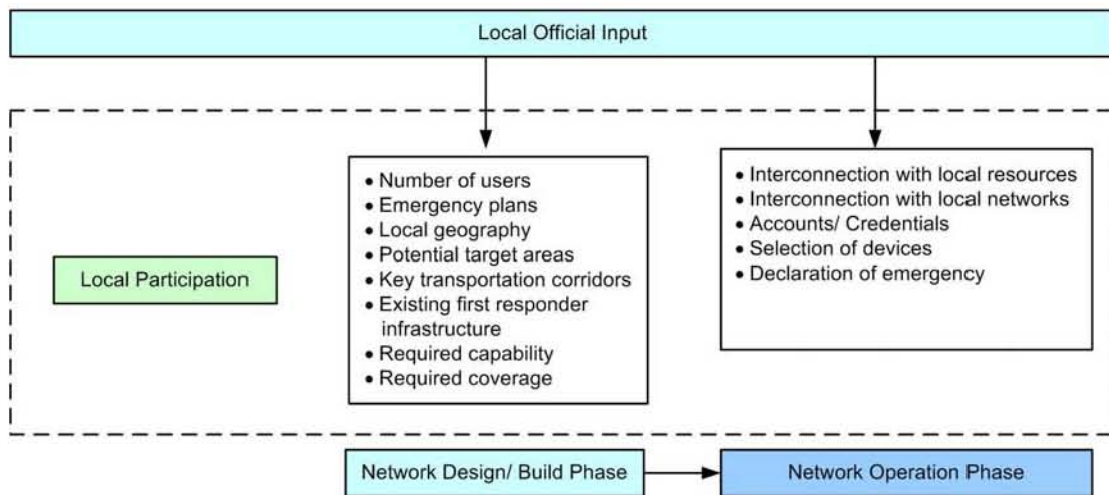
III. There Must be a Mechanism for Local Decision-Making on Technical/ Engineering Matters

Because the vast majority of first responders are local, the designers, implementers, and operators of public safety broadband wireless network should pay close attention to their needs. Moreover, nearly all emergencies are local. Even in national or regional emergencies, almost all communications will terminate within the locality or the state. Although the mission is similar across jurisdictions, the individual departments and jurisdictions vary in scale, density, climate, environment, and internal resources. Urban jurisdictions may have a range of ongoing surveillance requirements and large numbers of mobile staff. Rural areas may have a few individuals covering hundreds of square miles, but may obtain backup from state and local authorities.

Some jurisdictions may have considerable internal expertise and funding and existing network infrastructure. Others may not have funds or expertise or a clear sense of their requirements. In either case, any jurisdiction may be the location of an emergency, and the network must “work” well anywhere.

There should be a well-considered, structured process of incorporating local decision-making and guidance on technical and engineering matters. At the outset of the design process, local first responders must be brought into the process. The designers of the network must work with the requirements of the individual community, including likely number of users, emergency plans, local geography, potential target areas, key transportation corridors, and existing first-responder infrastructure. Figure 4 illustrates two phases of network design/build and network operation.

Figure 4: Phases in Network Design/Build and Network Operation



In the event the local jurisdictions have little expertise or infrastructure to contribute, coordination is still necessary to determine the local first responder needs. In that case the network designer may perform the design and implementation using public safety best practices and lessons learned from implementations in comparable jurisdictions.

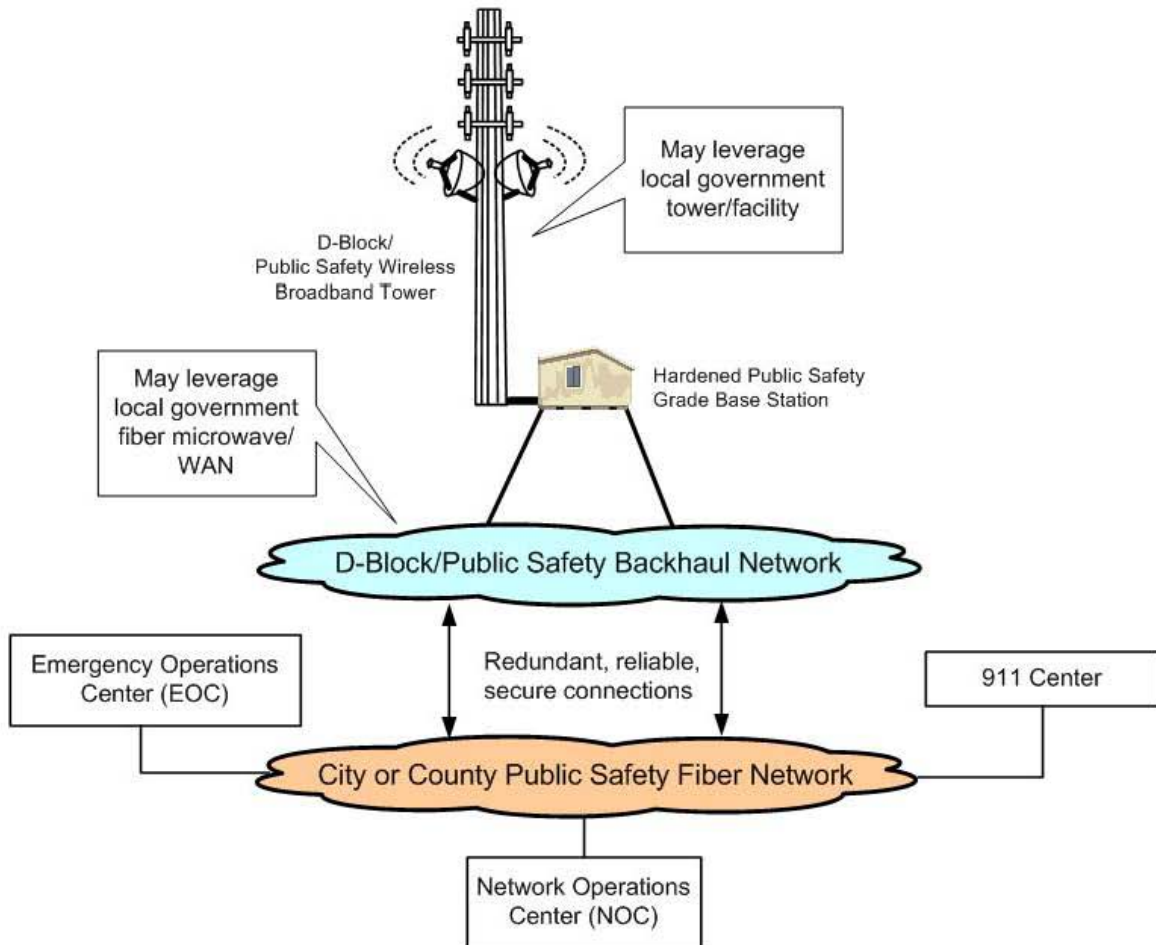
There is a range of areas that local first responders would need to coordinate to make effective use of the public safety broadband network:

A. Connectivity between the wireless network and the first responder network

The wireless network would require a reliable high capacity trunked connection to the resources of first responders. These include computer assisted dispatching (CAD) and records management systems (RMS), geographic information systems (GIS), file servers, criminal databases, emergency operations centers, local government Internet access, state and federal criminal information networks, national health and hazardous materials databases. The local government networks may include narrowband radio systems, other wireless networks such as WiFi and 4.9 GHz, and local fiber and microwave networks. The connectivity must be sufficiently high-capacity and reliable and use standards-based technologies. It must be secure, so as not to compromise the existing resources or operations. It must be an option for the local community to choose the means of connection; for example, redundant direct connections from the network to a county fiber network that bypasses the public Internet. Conversely, small communities with limited resources should have the ability to make a low-cost connection between its resources and the wireless network, potentially by way of point-to-point wireless connections or leased capacity.

Figure 5 illustrates the public safety grade broadband network facility.

Figure 5: Public Safety Grade Broadband Network Facility

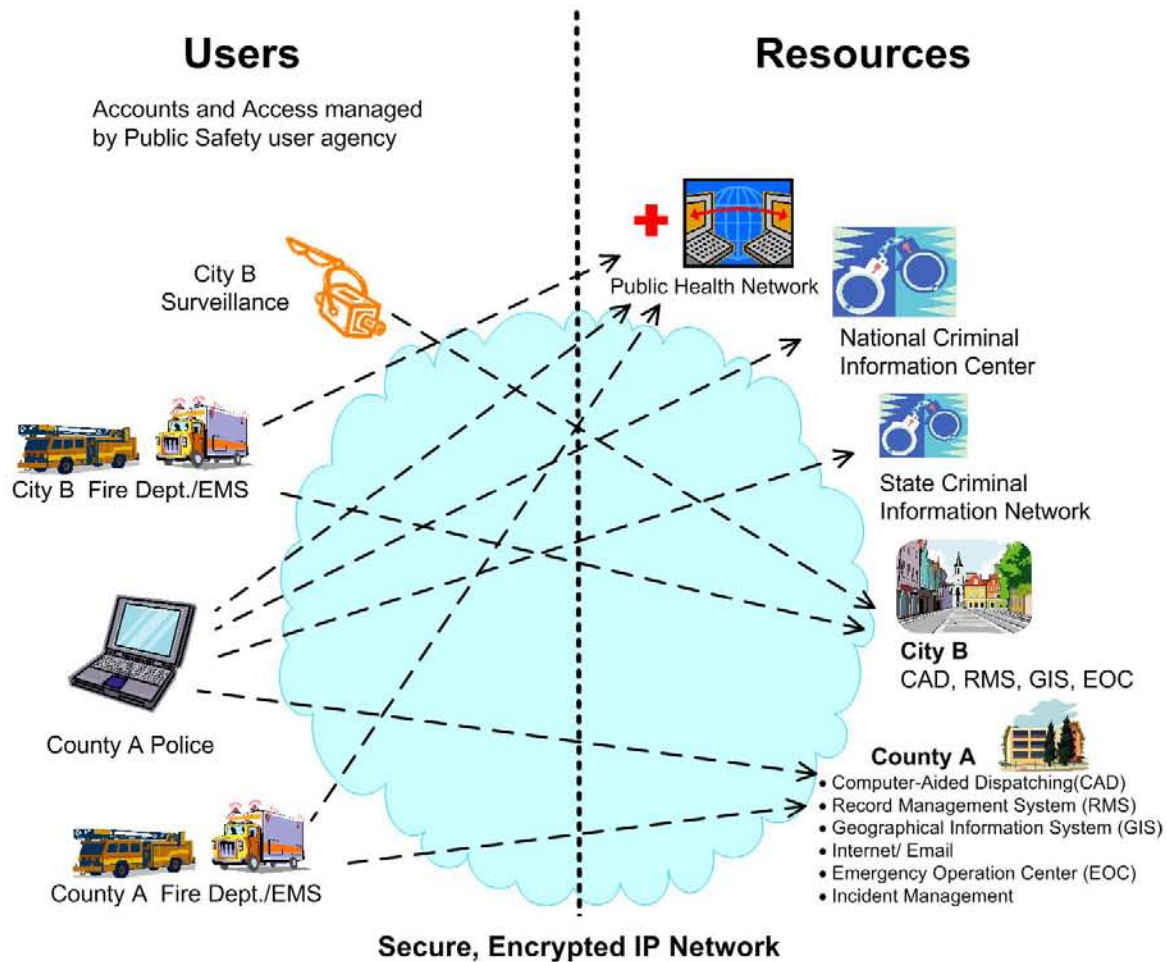


B. Control of access and authentication and security

Because the network must be secure, only authorized individuals should be able to use the network as authorized public safety users. There must be strict controls that ensure that unauthorized parties are not able to gain access as public safety users, and that users only have access to resources and networks to which they are authorized. For example, a user from a particular county would be authorized to have access to the network with a particular set of privileges and priorities, and furthermore that individual would be able to reach the authorized resources of that county through the network.

Figure 6 illustrates how users can access shared and dedicated resources over the public safety broadband network.

Figure 6: Utilization of Public Safety Broadband Network



Local first responders must have the ability to control and modify the network access privileges of all users, because local first responders manage the credentials and privileges of those individuals. This includes account management, the ability to activate and deactivate devices, and the ability to link particular accounts to particular devices. Account changes must be possible 24 hours a day and on demand, such as when a device is stolen or compromised.

C. Local first responder selection of devices

In order to maximize the breadth of innovation and minimize costs, local public safety entities should be able to select any device that meets the technological standard of the network and is certified to comply with the standard and not harm the network. This range of choice is far superior to an environment where the spectrum licensee works only with a particular subset of equipment manufacturers and controls the evolution of the user devices. Desirable examples of technology standards adopted in other areas include WiFi

wireless equipment and DOCSIS cable equipment, which are relatively inexpensive and developed by entrepreneurs independent of service providers.

Local public safety entities should be able to select devices based on a range of operational criteria, including their anticipated need (such as mobile data, voice, surveillance), the types of devices they wish to use (such as Personal Data Assistants, rugged radios, laptops, mobile routers), and their existing base of technology (for example, dual-mode 700 MHz/4.9 GHz networks may be desirable if the jurisdiction has a private wireless network).⁷ The criterion should be compatibility with the industry standard, so that the relation between the device and the core network is consistent, and the device does not interfere with the operation of the network.

D. Local first responder selection of applications

The public safety network must be able to serve a range of existing and unanticipated public safety challenges. Current public safety applications are known, and others are anticipated for the future. However, other innovations may emerge, and the network must be able to support those capabilities, as long as it is not unreasonably expensive to do so and as long as the new applications do not interfere with other critical applications. For example, innovations in virtual presence or in remote sensing/tracking of people in buildings and concealed areas may lead to developments of new imaging systems that may be transported over the network.

The local public safety entities should be able to determine whether and how to add new applications to the network and should not face exclusions of particular types of communications from the service provider. Where significant increases in usage may unduly affect the other uses and applications, the service provider should work with the public safety entities to determine the potential impact of the application and determine a strategy to implement it, including enhancement to the network and mutually agreed limitations on the use of particular applications.

⁷ The 4.9 GHz spectrum refers to that spectrum that has been allocated by the FCC for fixed and mobile wireless services as the designated band for support of public safety. "FCC Designates 4.9 GHz Band For Use in Support of Public Safety and Proposes Licensing and Service Rules," http://www.fcc.gov/Bureaus/Wireless/News_Releases/2002/nrw10202.html, accessed June 15, 2008. Significantly, however, the spectrum located at 4.9 GHz is far inferior to that at 700 MHz because of the need for line of sight connections. This requires much greater cell density and related network expense. A network in the 4.9 GHz band requires up to 10 times as many nodes as does a 700 MHz network. Telephony Online, "FCC OKs Public Safety Request for 4.9 GHz Mask," http://telephonyonline.com/news/web/telecom_fcc_oks_publicsafety/, accessed June 15, 2008.

E. Local determination of an emergency

In a particular region, the local emergency managers must be able to determine what constitutes an emergency requiring priority use of the public safety network. Almost all emergencies are local, and therefore the local emergency manager should be able to make this determination.

It has been pointed out that all public safety calls represent an emergency to someone, and that potentially the ability to override will result in frequent interruption of commercial users when it is not warranted. At the other extreme is the national Emergency Alert System (formerly Emergency Broadcast System), which enables the President to override all broadcasters and cable systems to speak to the public. It has never been used, not even on September 11, 2001.

To facilitate public safety, the network must work effectively for first responders and save lives. There are routinely emergencies with massive life-affecting local impact (tornadoes, floods, manhunts) that are never known to the nation as a whole. If the local emergency official determines that additional communications spectrum is needed to perform the job, it should be within the latitude of that individual to make the choice without intervention of a state or national official—and without resistance from the D Block licensee.

There may be technological solutions to the problem; for example, a priority scheme that, rather than entirely terminating the commercial use of the spectrum, would instead allocate additional capacity to public safety as needed, perhaps only partially reducing the non-public safety capabilities of the network, depending on the scale of the emergency. Moreover, the geographic reach of the reallocation could be limited to the area where first-responder activity was expected to be most intense.

IV. Expeditious Adoption of Open Standards Will Enable Efficiencies, Cost Savings, and Local Deployment Without Delay--and Without Compromising Interoperability

One of the key ways to make the spectrum useful to public safety users will be to adopt a standardized interoperable technology specification governing key features such as protocols, authentication, and use of channels in the spectrum. Regardless of whether the solution is a public private partnership or is public safety-financed, the selection of an industry standard will enable jurisdictions and equipment manufacturers to plan network deployments and begin to make interoperable equipment available.

As discussed above, there should be wide latitude in public safety agencies' ability to select devices. However, networks can only be cost-effectively and quickly implemented when there is clarity in the technical standards and in how the network will operate.

Even if there is no single national initiative, the adoption of an industry standard for the spectrum will enable devices to work in any part of the U.S., regardless of how they are managed or financed. First responders and their devices will be able to seamlessly roam to any part of the U.S. It will create a Level 6 Interoperability System according to U.S. Department of Homeland Security standards,⁸ immediately creating the highest attainable level of data network interoperability among its users.

Adoption of a technical standard will enable pending local efforts to proceed without delay and without risk to interoperability. It will enable first responders to be prepared in the event of an emergency and enable public safety agencies to begin to migrate from less interoperable, less reliable, commercial networks.

Further, selection of an open standard, with silicon chips and components in common with widely adopted commercial technologies, will keep device costs low. As an illustration, conventional WiFi hotspot access points have fallen from over \$500 per unit to \$20 per unit in the past eight years of adoption and the sale of tens of millions of devices. In contrast, proprietary public safety push-to-talk radios are manufactured in tens or hundreds of thousands and cost thousands of dollars, despite the fact that they are essentially hardened cellular telephones. Through standardization, devices will become far more affordable for public safety agencies throughout the U.S., a benefit that will also accrue to commercial users.

V. Combined Spectrum Will Boost Spectral and Cost Efficiencies

Keeping 22 MHz of spectrum together is advisable from a technical standpoint, regardless of the business plan selected.

The combination of the spectrum in the public safety broadband and D Block spectrum enables more efficient use of spectrum and other technical resources. There are several reasons why this is a technical benefit:

- a. It's a significant advantage to *commercial* D Block customers—they will be receiving services from a public safety grade network that is clearly superior

⁸ Level 6 Interoperability is also known as Standards-Based Radio System or "Project 25." It enables over-the-air and wireless communications through shared systems that depend on open standard functionality. Two open air interface standards exist in the US. "Texas Radio Communications Interoperability Plan," Texas Department of Public Safety <http://www.txdps.state.tx.us/dem/documents/texasradiocomminteroperabilityplan.doc>, accessed June 15 2008.)

to other commercial networks because it was designed to meet first responder needs.

- b. Operating a single network in the spectrum will enable a greater body of users to benefit from the antennas, radios, towers, and backhaul systems that will need to be built. If there were separate commercial and public safety networks in the 22 MHz of spectrum, approximately twice the cost of infrastructure would be necessary to make it operate. Efficiency arises from the sharing, by commercial and public safety networks, of a single platform with a single set of antenna structures, base stations, backhaul, management systems, and RF designers.

If a service provider must build a new network to activate a separate channel band, the cost of the activation may be millions or tens of millions of dollars in a single metropolitan area. Carrier broadband wireless architectures may require base stations every 1.5 kilometers. Individual base station costs vary widely depending on environment and the needs of a particular area, but are on the order of magnitude of \$100,000, plus ongoing lease fees. Backhaul costs are significant, with \$50,000 to \$150,000 required to build a mile of fiber optic cable, or thousands or tens of thousands of dollars per month required to lease comparable capacity from a service provider.

- c. A joint buildout will result in less impact to the public rights-of-way because fewer towers, antennas, microwave infrastructure, and/or fiber infrastructure would need to be constructed.
- d. Larger spectrum blocks enable operation with large channel bandwidths and high power—making it possible for devices to attain a given speed with fewer towers, each serving a larger area. This type of operation is particularly suitable for blanketing a larger geographic area, as would be necessary to cover rural areas.
- e. Larger blocks of spectrum increase the flexibility for serving areas near international borders. King County, WA, for example, has noted the extreme difficulty of operating a wireless network in a major U.S. metropolitan area (Seattle) that adjoins a major Canadian metropolitan area (Vancouver)—and in which each of these networks must share spectrum with the other, a situation not faced in much of the rest of the U.S.
- f. If, instead, two adjacent, non-coordinated networks operate in the aggregate 22 MHz, the spectrum allocation will require a guard band between the two allocations, which are currently not separated by a guard band on the assumption that the two blocks will be operated as a whole. Adding a guard band will entail decreasing the allocation of spectrum to the D Block. There will result a greater loss of spectrum use, because of the need for guard bands and mitigation of RF interference among the many individual providers/bands.

VI. Verification of Public Safety Compliance Will Be Essential

The requirement for compliance with public safety requirements of the public/private partnership is literally a matter of life and death. Public safety entities will potentially have much less hands-on control than in their existing networks. There must be a vigorous and transparent mechanism for identifying and enforcing these requirements. It should be made clear in the rules for the spectrum that the FCC will be paying close attention. Either in the rules or early in the development of the network, a penalty level should be determined for missing development milestones, missing deployment deadlines, and failure to meet capacity, coverage, and reliability requirements. There should be a formal mechanism for independently verifying that capacity, coverage, and reliability fulfill the requirements of public safety.

As the network becomes operational, independent testing should continue, as well as enforcement and penalties regarding capacity, coverage, and reliability. There should be regular tests of the prioritization scheme. There should be penalties in the event that traffic prioritization does not operate as required, or in the event that the private partner does not adequately respond to a prioritization request by an authorized official. The security and authentication systems should be regularly tested. User and agency complaints should be logged and reviewed regularly by an oversight entity. Finally, there should be a mechanism for requiring the private partner to address ongoing limitations and problems with the network and perform remedial activity or enhancements as necessary. Absent verification, risk exists of mistaken or intentional abrogation of public safety requirements.